

WILLKIE FARR & GALLAGHER LLP
BENEDICT Y. HUR (SBN: 224018)
bhur@willkie.com
SIMONA AGNOLUCCI (SBN: 246943)
sagnolucci@willkie.com
EDUARDO E. SANTACANA (SBN: 281668)
esantacana@willkie.com
ARGEMIRA FLÓREZ (SBN: 331153)
aflorez@willkie.com
HARRIS A. MATEEN (SBN: 335593)
hmateen@willkie.com
RODOLFO E. RIVERA AQUINO (SBN: 348512)
rriveraaquino@willkie.com
333 Bush Street, 34th Floor
San Francisco, CA 94104
Telephone: (415) 858-7400

Attorneys for Defendant
GOOGLE LLC

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

ANIBAL RODRIGUEZ, *et al.* individually and on
behalf of all others similarly situated,

Plaintiff,

v.

GOOGLE LLC, *et al.*,

Defendant.

Case No. 3:20-CV-04688 RS

**REPLY IN SUPPORT OF GOOGLE
LLC'S MOTION FOR SUMMARY
JUDGMENT**

Date: July 25, 2024
Time: 1:30 p.m.
Courtroom: 3, 17th Floor
Judge: Hon. Richard Seeborg

Action Filed: July 14, 2020
Trial Date: February 10, 2025

TABLE OF CONTENTS

I.	Introduction.....	1
II.	This Court should determine the consent question on the undisputed record.	2
A.	The underlying facts establishing that Google secured consent through its Privacy Policy are not in dispute.	2
B.	The WAA control did not withdraw consent for pseudonymous record-keeping or pseudonymous analytics account servicing.	3
C.	Plaintiffs fail to raise a material dispute concerning whether Google maintains (s)WAA-off data in pseudonymous form.	6
D.	Once rhetoric is set aside, Plaintiffs do not dispute that Google never used WAA-off data to personalize advertising or build marketing profiles.	8
E.	No internal employee agreed with Plaintiffs’ interpretation of WAA.....	9
III.	Plaintiffs cannot establish a reasonable expectation of privacy, intent, or highly offensive conduct.	11
IV.	Plaintiffs cannot establish harm.	13
VI.	Conclusion	16

TABLE OF AUTHORITIES**Page(s)****Cases**

<i>Brown v. Google LLC</i> , 2023 WL 5029899 (N.D. Cal. Aug. 7, 2023)	12
<i>Campbell v. Facebook, Inc.</i> , 951 F.3d 1106 (9th Cir. 2020)	11, 12
<i>Dinerstein v. Google, LLC</i> , 73 F.4th 502 (7th Cir. 2023)	6
<i>Doe 1 v. AOL LLC</i> , 552 F.3d 1077 (9th Cir. 2009)	3
<i>Eichenberger v. ESPN, Inc.</i> , 876 F.3d 979 (9th Cir. 2017)	6
<i>Ellsworth v. Schneider Nat'l Carriers, Inc.</i> , 2021 WL 6102514 (C.D. Cal. Oct. 28, 2021).....	15
<i>Gadomski v. Patelco Credit Union</i> , 2022 WL 223878 (E.D. Cal. Jan. 25, 2022)	15
<i>In re Google RTB Consumer Priv. Litig.</i> , 606 F. Supp. 3d 935 (N.D. Cal. 2022)	7
<i>In re Google, Inc. Privacy Pol'y Litig.</i> , No. 5:12-CV-001382-PSG, 2015 WL 4317479 (N.D. Cal. July 15, 2015).....	13
<i>Graham v. Noom, Inc.</i> , 533 F. Supp. 3d 823 (N.D. Cal. 2021)	2
<i>Hammerling v. Google, LLC</i> , 615 F. Supp. 3d 1069 (N.D. Cal. 2022)	3, 12
<i>I.C. v. Zynga, Inc.</i> , 600 F. Supp. 3d 1034 (N.D. Cal. 2022)	13
<i>In re iPhone Application Litig.</i> , 844 F. Supp. 2d 1040 (N.D. Cal. 2012)	13
<i>Love v. Ladder Fin., Inc.</i> , 2024 WL 2104497 (N.D. Cal. May 8, 2024)	2
<i>Low v. LinkedIn Corp.</i> , 900 F. Supp. 2d 1010 (N.D. Cal. 2012)	6, 12, 13

1	<i>Massie v. Gen. Motors LLC</i> ,	
2	No. CV 21-787-RGA, 2022 WL 534468 (D. Del. Feb. 17, 2022)	13
3	<i>McClung v. AddShopper, Inc.</i> ,	
4	2024 WL 189006 (N.D. Cal. Jan. 17, 2024)	14
5	<i>McCoy v. Alphabet, Inc.</i> ,	
6	2021 WL 405816 (N.D. Cal. Feb. 2, 2021)	12, 13
7	<i>Spokeo, Inc. v. Robins</i> ,	
8	578 U.S. 330 (2016)	13
9	<i>Wesch v. Yodlee, Inc.</i> ,	
10	2021 WL 1399291 (N.D. Cal. Feb. 16, 2021)	12
11	<i>Williams v. What If Holdings, LLC</i> ,	
12	No. C. 22-03780 WHA, 2022 WL 17869275 (N.D. Cal. Dec. 22, 2022)	2, 12
13	<i>Winsor v. Sequoia Benefits & Ins. Servs. LLC</i> ,	
14	No. 21-CV-00227-JSC, 2021 WL 5053087 (N.D. Cal. Nov. 1, 2021)	15
15	<i>In re Zynga Priv. Litig.</i> ,	
16	750 F.3d 1098 (9th Cir. 2014)	13
17	Statutes	
18	Cal. Civ. Code § 1798.140(v)(1)	7
19	Cal Civ. Code § 1798.140(v)(3)	6, 7
20	Other Authorities	
21	BAJI 7.26 (2024)	14
22	CACI 1820 (2024)	14
23	Rule 23(b)(3)	2
24		
25		
26		
27		
28		

I. Introduction

Google should prevail on summary judgment because the undisputed facts show: (1) Plaintiffs consented to the remaining challenged practices; (2) those practices were not highly offensive; and (3) Plaintiffs suffered no legally cognizable harm.

Plaintiffs consented. The undisputed facts show that Plaintiffs consented to the only two practices they still challenge: Google servicing Google Analytics accounts with pseudonymous app activity data, and Google pseudonymously logging ad service for basic recordkeeping. *First*, in certifying the Class, this Court ruled that the parties can assume app developers secured consent from all class members for their apps to use Google Analytics pursuant to Google’s terms. *See* Dkt. 109, at 10-11. The WAA button never promised that users could disable Google’s basic servicing of analytics accounts. It stated only that toggling it off would prevent data from being “saved to your Google Account”—a promise Google indisputably kept.

Second, Plaintiffs consented to Google’s Privacy Policy, which disclosed pseudonymous recordkeeping. Toggling the WAA button did not revoke that consent because the WAA button never mentioned that it withdraws Google’s right to keep a de-identified record of its ads serving. No reasonable interpretation of WAA’s limitation “saved to your Google Account” would cover data that is *not* saved to a Google Account.

Third, even if the Named Plaintiffs prove they were confused about the ambit of the WAA control, such confusion would undermine their claims of class-wide consent. Google secured unambiguous consent for pseudonymous record-keeping and servicing analytics accounts. Without a clear and unambiguous withdrawal of that consent, Google should not be held liable.

Google’s conduct was not highly offensive. Even if the Court finds the WAA language ambiguous, Plaintiffs’ invasion of privacy claims still fail because there is no reasonable allegation that Google’s conduct was highly offensive. It is undisputed that (i) Google intentionally designed its systems to de-identify (s)WAA-off, data based on Google’s understanding of its disclosure; and (ii) Google only uses this de-identified data for receipts of ads served and to service analytics accounts, and never uses (s)WAA-off data to personally identify individuals. This type of pseudonymous record-keeping cannot be an egregious breach of social

1 norms.

2 ***Plaintiffs suffered no actual harm.*** Invasion of privacy and CDAFA claims require an
3 actual harm—a higher bar than Article III standing, and Plaintiffs come nowhere close to clearing
4 it. Google’s practice of keeping pseudonymized records to account for served ads harms no one.
5 Nor does Google’s servicing of analytics accounts for app developers—who are required to (and
6 do) disclose that they analyze their users’ activities and may use Google to store and process that
7 information.¹ *See, e.g.,* MSJ App’x. A-2 (Sample of Historic GA4F Terms of Service), Dkt. 383-
8 2, at 40. App developers choice to use Google for this purpose causes no harm, because Google
9 shields users’ identities when (s)WAA is off. And besides, Plaintiffs’ damages theory—used to
10 secure Rule 23(b)(3) certification—has no relationship to the servicing of analytics accounts,
11 anyway; it hinges entirely on Google’s ad service recordkeeping instead.

12 Plaintiffs’ real argument comes near the end of their opposition: even if the Court accepts
13 every one of Google’s arguments, it must still deny summary judgment because mobile devices
14 are “necessities, not luxuries,” so therefore, no one could voluntarily consent to collection of *any*
15 mobile data. Opp., Dkt. 398, at 23. It does not matter to these Plaintiffs what Google discloses,
16 where, or how; they would still argue they’re entitled to a half billion dollars in damages.

17 **II. This Court should determine the consent question on the undisputed record.**

18 **A. The underlying facts establishing that Google secured consent through its 19 Privacy Policy are not in dispute.**

20 This Court’s ruling granting class certification accepted Plaintiffs’ argument that “express
21 consent does not defeat predominance because the ‘sWAA disclosures and Google’s Privacy
22 Policy’ are the only relevant materials for analysis, and are ‘the same for all class members.’”
23 Class Cert. Order, Dkt. 352, at 15 (quoting Class Cert. Reply, at 15). The content of these
24 documents is undisputed. And it is undisputed that the Privacy Policy (“PP”) disclosed and

25 ¹ Courts have repeatedly held no such liability arises just from servicing analytics accounts. *See,*
26 *e.g., Love v. Ladder Fin., Inc.*, 2024 WL 2104497, at *2 (N.D. Cal. May 8, 2024) (“[T]hat
27 [analytics provider] records and stores for [website’s] own use information that users have
28 voluntarily shared with [website] . . . is not the kind of privacy intrusion that California’s
constitution bars.”); *Graham v. Noom, Inc.*, 533 F. Supp. 3d 823, 833 (N.D. Cal. 2021); *Williams*
v. What If Holdings, LLC, No. C. 22-03780 WHA, 2022 WL 17869275, at *3 (N.D. Cal. Dec. 22,
2022).

1 secured consent for Google to service analytics accounts and keep pseudonymous records of ads
2 served and conversions. *See* Mot., Dkt. 383, § III.C.

3 Plaintiffs dispute Google’s undisputed material **Facts 1** and **4** even though they simply
4 reproduce Google’s disclosures. *See* Opp., Dkt. 398, at 3. And they dispute that the phrase “saved
5 to your Google Account” was limiting (**Fact 2**), even though by its plain terms it must be. They
6 further dispute that the PP explained that “associated with your Google Account” and “associated
7 with your personal information” are synonymous. (**Fact 3**). But the text of these documents is not
8 in dispute, and as such, the Court can determine their meaning for itself. No jury is required to
9 understand the plain meaning, nor does the subjective confusion of a named Plaintiff matter if the
10 plain meaning is unambiguous. *See, e.g., Doe I v. AOL LLC*, 552 F.3d 1077, 1081 (9th Cir. 2009)
11 (“[T]hat the parties dispute a contract’s meaning does not render the contract ambiguous.”).

12 **B. The WAA control did not withdraw consent for pseudonymous record-keeping**
13 **or pseudonymous analytics account servicing.**

14 Plaintiffs’ brief confuses the consent issue. It is undisputed that Plaintiffs provided consent to
15 Google receiving GA4F data, servicing the analytics accounts of third-party app developers, and
16 keeping pseudonymous records of ad service. *See* Mot., Dkt. 383, § III.C; *Hammerling v. Google,*
17 *LLC*, 615 F. Supp. 3d 1069, 1090 (N.D. Cal. 2022), *aff’d*, No. CV-22-17024 (9th Cir. Mar. 5,
18 2024) (unpublished). The consent question on each of Plaintiffs’ claims is whether they
19 unambiguously and expressly *withdrew* their consent to those activities by switching the (s)WAA
20 control to “off.” This distinction matters. Only a clear, express *withdrawal* of consent for one of
21 these activities could undo the clear, express consent for them. Plaintiffs argue that they
22 interpreted the WAA button to control consent over *all* data collected through GA4F, whether or
23 not it is “saved to your Google Account.” That interpretation cannot square with any reasonable
24 reading of the WAA disclosure or of Google’s Privacy Policy.

25 First, Plaintiffs claim they withdrew consent because Google never disclosed that
26 pseudonymized collection would still occur when (s)WAA is off. That is circular. By their logic,
27 all privacy buttons Google makes available to its users withdraw consent for all activities unless
28 expressly stated otherwise. It cannot be that Google’s disclosures must not only list the ways a

1 button will change its practices, but also every way it *will not*.

2 Simultaneously, Plaintiffs excise the critical limitation in WAA’s language every time they
3 mention it: “saved to your Google Account.” *See* Opp., Dkt. 398, at 3:8, 5:13, 5:16, 11:17, 11:21.
4 They even complain that users, in Google’s view, have “no power to stop Google from collecting
5 and using app activity data.” Opp., Dkt. 398, at 6:3-6. But Google never made this promise;
6 Plaintiffs simply ignored the clear limitations within the WAA disclosure.²

7 When they finally do address the “saved to your Google Account” limitation, Plaintiffs
8 stretch in their attempt to bend around it. They argue that Google never “disclosed to users that the
9 company collects and saves data *in* other places that Google does not consider to be their ‘Google
10 Accounts.’” But what else could “saved to your Google Account” mean? Per Plaintiffs, the
11 language means nothing without an accompanying additional disclosure that there is such a thing
12 as “*not* your Google Account.” This is part and parcel of the increasing absurdity presented by
13 these privacy class actions, which are often based on an allegation that defendants have confusing
14 disclosures and privacy policies even as they claim the privacy policy should be larded up with
15 sentence after sentence disclaiming the particular practice that the plaintiff happens to sue over.
16 Common sense and the plain meaning of the language in question must prevail here.

17 In pushing their strained interpretation of WAA, Plaintiffs likewise avert their gaze from
18 the Privacy Policy’s clear and explicit language: just after explaining that Google collects
19 analytics and advertising data, it says that “[i]nformation we collect when you are signed in to
20 Google, in addition to information we obtain about you from partners, may be associated with
21 your Google Account. *When information is associated with your Google Account, we treat it as*
22 *personal information.*” MSJ App’x A-7 (Privacy Policies), Dkt. 383-2, at 5. And it promises *only*
23 that users “*can access, manage or delete information that is associated with your Google*
24 *Account*” by “visit[ing] the Transparency and choice section of this policy,” which is where
25 Google describes the WAA control. Nowhere does Google promise that users can also “access,
26

27 ² That Google makes general representations that it has various controls telling users that they can
28 control the data Google collects and saves is irrelevant. *See, e.g.,* Opp., Dkt. 398, at 13:21-27 & 5
n.4. Obviously this does not mean that every bit and byte is subject to a toggle, and the specific
description of each toggle (like the one Plaintiffs’ case hinges on) controls what it should do.

1 manage or delete information that is *not* associated with your Google Account.” The Opposition
2 fails to address this language entirely. *See* Opp., Dkt. 398, at 14:27 (focusing only on unrelated
3 language).

4 Plaintiffs’ strained interpretation further relies on a long disproven theory. They argue that
5 this Court already decided the term “Google Account” is confusing. But they ignore that the Court
6 was presented with an entirely different case then. At the time, Plaintiffs *alleged* that Google used
7 (s)WAA-off GA4F data to personalize advertising and build marketing profiles, in contravention
8 of the description of WAA. Google could not argue then that Plaintiffs’ allegations were false.
9 Now that they are proven false, Plaintiffs’ theory casts a shadow of a far different hue. Even if a
10 reasonable juror could find that keeping and using marketing profiles in a digital bucket that
11 Google labeled “not your Google Account” violated the description of WAA, no reasonable juror
12 can conclude that de-identifying analytics data and receipts of ad service is equivalent to
13 “sav[ing]”app activity data “to your Google Account.”

14 Plaintiffs argue that each named Plaintiff “interpreted the Google disclosures to mean that
15 Google would not collect or save their app activity data when (s)WAA was off” (ignoring the
16 limitation “saved to your Google Account”), Opp., Dkt. 398, at 11:21-24, and that even if Google
17 is right about everything, the “user would reasonably believe that the activity data Google
18 collected, stored, and linked to unique, personal identifiers, was part of that user’s Google
19 Account,” *id.* at 11:21-23, 15:7-9. Here again, Plaintiffs read the limitation out of the WAA
20 control, rendering it surplusage. If all data collected with an identifier is reasonably considered
21 “part of that user’s Google Account,” then the phrase doesn’t limit the WAA button at all, and the
22 phrases in the Privacy Policy distinguishing personal from non-personal information would mean
23 nothing, either.

24 Named Plaintiff Cataldo revealed the absurdity of this position. He wanted Google to
25 serve him personalized ads using data Google collected when WAA was on. App’x A-17 (Cataldo
26 Dep. Tr.), Dkt. 383-2, at 298-299. This would be impossible under Plaintiffs’ view that Google
27 should “not save or use (s)WAA-off data at all, whether for ads or not.” Opp., Dkt. 398, at 14:3-4;
28 see also Mot., Dkt. 383, at 9 n.12 (“Google would not be able to serve an ad in those situations.”).

1 Plaintiffs’ certified theory of liability does not apply to Cataldo, who apparently did not have the
 2 same belief regarding Google’s practices that his counsel claim all class members had. This calls
 3 into question whether the certified theory of liability applies to Cataldo at all, and casts doubt on
 4 the notion that toggling WAA off represents a class-wide, express withdrawal of consent.

5 **C. Plaintiffs fail to raise a material dispute concerning whether Google maintains**
 6 **(s)WAA-off data in pseudonymous form.**

7 Plaintiffs use phrases like “digital fingerprint” to describe the GA4F data that app
 8 developers send to Google, thereby disputing Google’s **Facts 5, 6, and 7**. This is more semantic
 9 gymnastics. Plaintiffs do not dispute that Google erected a massive infrastructure designed to
 10 separate data tied to a user’s identity from data tied to pseudonymous identifiers.³ Google did not
 11 do that on a whim; it did it because it intended to and does maintain different digital silos
 12 depending on the various permissions users grant it, and uses the data in those silos differently
 13 depending on permissions. Plaintiffs’ gripe here is that Google’s attempts to separate data into
 14 these two silos are inadequate because there could be leakage or linkage from one to the other.

15 *To be clear: Plaintiffs identified no evidence of any such leakage* ever occurring in
 16 connection with any particular class member. Their concern is purely theoretical, and litigants are
 17 not held liable for conduct they *could* engage in. The inquiry on this subject should end there.

18 In one sentence, Plaintiffs expressly accuse Google of tying pseudonymous IDs to users’
 19 GAIA IDs by quoting their expert, who explains correctly that Google uses GAIA ID to *check for*
 20 *the user’s consent* before further processing the GA4F data. Opp., Dkt. 398, at 12:19-21. In other
 21 words, in an ironic twist, *Plaintiffs fault Google for checking the WAA setting of the user* so it can

22
 23 ³ For example, a device ID is meaningless without some other piece of identifying information,
 24 and that “something more” is what Google keeps apart from device ID. *See* Opp., Dkt. 398, at 12;
 25 *see also Eichenberger v. ESPN, Inc.*, 876 F.3d 979, 980 (9th Cir. 2017) (device serial number does
 26 not constitute “personally identifiable information” under the VPPA). The CCPA recognizes this
 27 exact concept. *See* Cal Civ. Code § 1798.140(v)(3) (discussing pseudonymization of data); *see*
 28 *also Dinerstein v. Google, LLC*, 73 F.4th 502, 513-14 (7th Cir. 2023) (anonymized medical
 records lacking direct patient identifiers do not give rise to a concrete Article III injury, even if
 there are potential technical means to re-identify the records, absent plausible allegations that the
 records actually have been re-identified); *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1025
 (N.D. Cal. 2012) (no invasion of privacy through disclosure of unique “LinkedIn ID” and
 browsing activity even when one could “through inferences, de-anonymize this data[.]”).

1 determine how the data should be treated. And Plaintiffs leave out that Google strips the data of
2 the GAIA ID when (s)WAA is off before saving it to memory. *See* Mot., Dkt. 383, at 15:13-16:15.

3 Plaintiffs also claim repeatedly that Google can “connect data collected while (s)WAA was
4 off to individual users’ personal identities” because in this litigation “Plaintiffs requested
5 discovery pertaining to the (s)WAA-off data collected under their names and/or device identifiers
6 and received troves of data tied to the very same.” Opp., Dkt. 398, at 18:1-6; *see also id.* at 8:1-2.
7 That grossly distorted claim cites to Plaintiffs’ technical expert’s report, which instead explains
8 what *actually* happened: “*the named Plaintiffs provided* Google identifiers obtained from their
9 Android devices to Google, *allowing* Google to search for and produce their data from within
10 Google’s Analytics storage infrastructure.” Hochman Rpt., Dkt. 398-5, ¶ 178 (emphasis added).
11 That distinction is everything: Google did not “connect” anything; it was Plaintiffs who did the
12 connecting, by, in the flesh, looking up their own device IDs while holding their own phones and
13 providing those identifiers to Google. Santacana Reply Decl. ¶¶ 3-4.

14 In the absence of evidence undermining the fact that Google designed its infrastructure to
15 separate pseudonymous data from users’ true identities, Plaintiffs rely on misleading quotations
16 from two internal documents. First, Plaintiffs rely on Mao Exhibit 34, even though they know
17 from deposition testimony that the comment they rely on regarding eroding the barriers between
18 pseudonymous IDs and GAIA ID was a comment *hypothesizing* on the downsides of a technical
19 proposal that *Google never adopted*, in part because of those downsides. *See* Santacana Dec. at
20 Ex. G (Ganem Dep. Tr.) at 260-61. And they quote a seven-word phrase “Can be blocked from
21 joining PII with ID?” from Mao Exhibit 33, Dkt. 398-34, a 50-page presentation. Despite its
22 apparent critical relevance to Plaintiffs’ case, Plaintiffs never asked any of the fourteen Google
23 witnesses they deposed about it, and there is no explanation of what it means in the document.
24 What it certainly does not mean is that Google uniformly, or in any way, joins PII to Android Ad
25 ID (AdID). *See* Mot., Dkt. 383, §§ III.D., III.E. If that was Google’s class-wide practice, Plaintiffs
26 would cite to actual evidence of that, but they have cited no such evidence.⁴

27
28 ⁴ Plaintiffs overstate *In re Google RTB Consumer Priv. Litig.*, 606 F. Supp. 3d 935 (N.D. Cal. 2022), which did *not* hold that these identifiers are personally identifying. There, the court

D. Once rhetoric is set aside, Plaintiffs do not dispute that Google never used WAA-off data to personalize advertising or build marketing profiles.

In another effort to undermine Google’s consent argument, Plaintiffs purportedly dispute that Google never used (s)WAA-off data to personalize advertising or build marketing profiles, which would arguably contradict the WAA button description. But every expert in this case agreed that Google told the truth from the start: Google does not personalize advertising or use marketing profiles using (s)WAA-off GA4F data. *See* Mot., Dkt. 383, at 8:12-9:3 & n.10. Just a few months ago, Plaintiffs agreed with that too. In the second paragraph of their class certification motion, Plaintiffs argued that “Google collects, saves, and uses (s)WAA-off data” and that “Google simply conceals that fact from users by (i) turning off ‘personalized’ ads that could tip them off to Google’s continued tracking” Class Cert. Mot., Dkt. 361-1, at 2:19-20.

Now, facing summary judgment, Plaintiffs reverse course again, disputing Google’s **Fact 8**, arguing with a straight face that selecting ads based in part on (1) the device’s **location**, (2) **which app** is requesting an ad be served (which they say can be used to infer “expressed interest” of the user), and (3) the **language** of the device constitutes “targeted advertising.” *See* Opp., Dkt. 398, at 4, 9:8-9. This is linguistic abuse. That is not in any way personalized advertising, nor is it targeting using “app activity data,” which is the only relevant type of data the WAA control is alleged to cover in this case. Indeed, right in between the two ranges of paragraphs from the Hochman Report that Plaintiffs rely on in disputing Fact 8 is their technical expert’s own concession that “Google does not use data collected by GA4F from WAA- and sWAA-off users to serve personalized ads.” Hochman Rpt., Dkt. 398-5, ¶ 278.

Plaintiffs’ brief does not identify a single instance of GA4F data being used to personalize advertising, despite four years of discovery and five months of expert discovery. And despite their pages of complaints about how rich analytics data can be, their actual claim of personalized advertising now apparently boils down to Google selecting ads based on which app asked for the

assumed that identifiers were joined with identifying information. Nor is Cal. Civ. Code § 1798.140(v)(1) helpful to Plaintiffs; section 1798.140(v)(3) excludes from “personal information” “consumer information that is deidentified or aggregate consumer information.” *See also id.* at 1798.140(aa) (defining “Pseudonymize”).

1 ad, roughly where the device is, and which language the ad should be in—core record data that
 2 cannot reasonably be considered “app activity data.” No one needed half a decade of litigation to
 3 demonstrate the unremarkable fact that Google does this; Google disclosed that in its PP
 4 throughout the class period. *See* App’x A-7 (PP), Dkt. 383-2, at 119 (disclosing categories of
 5 information that Google “automatically collect[s] and store[s] . . . in server logs.”).

6 Similarly, Plaintiffs argue that Google “creates comprehensive profiles of (s)WAA-off
 7 users’ app activity” because it keeps a log of ad service and ad conversions alongside
 8 pseudonymous identifiers that are never linked to a person’s true identity. *See* Mot., Dkt. 383, at
 9 9:10-12, 4:10. This kind of wordplay threatens to mislead the Court. Plaintiffs know that Google
 10 does not use these supposed “comprehensive profiles” to select advertising. *Id.* at 8. They are not,
 11 in fact, profiles at all. What they refer to here, from their cited evidence (Mao Ex. 4, Dkt. 398-5,
 12 Hochman Rpt., ¶¶ 279-82), is a “conversion log,” a table where every row represents a conversion
 13 event, and the columns list the pseudonymous ID that generated the event, the event’s ID, and the
 14 type of conversion so that the advertiser can understand how well their campaign performed
 15 (without enabling anyone to personally identify any particular user or target advertising).
 16 Hochman Rpt. at ¶ 236; *See also* Black Rpt. at ¶140. This obviously isn’t a marketing profile, but
 17 even if it were called that, it doesn’t matter, because Google doesn’t use it for marketing. It
 18 doesn’t select ads based on it. It doesn’t change a user’s experience or augment its understanding
 19 of any user in particular using it. It simply records that it happened, and tells the advertiser the
 20 tally. *See* Mot., Dkt. 383, at 8-9. Nothing in the Opposition disputes that, even as it purports to
 21 raise a dispute of Google’s Fact 8.

22 **E. No internal employee agreed with Plaintiffs’ interpretation of WAA.**

23 Plaintiffs lean on snippets that are out of context, disavowed, or inaccurate statements from
 24 some of Google’s over 150,000 rank-and-file. They do not raise a dispute of *material* fact, because
 25 the material facts—what Google said and what Google does—are undisputed.

26 First, Plaintiffs misrepresent Chris Ruemmler’s emails, as they have done many times,
 27 while ignoring his deposition testimony disavowing Plaintiffs’ preferred reading of them. Mr.
 28 Ruemmler doesn’t work in WAA, he works in Google Workspace (e.g., enterprise email accounts

and Google Docs), where “everything is GAIA tied.” Santacana Dec. at Ex. D (Ruemmler Tr.), at 61:16-20, 76:2-7. Based on this, he misunderstood internal, unrelated proposals at Google, and thought they would undermine the WAA button because he thought Google would GAIA-tie data even when WAA was off. *Id.* at 76. He was wrong about the proposals, and his fear was misplaced. After learning that other departments at Google, including Google Analytics, can and do “store” WAA-off data “anonymously” through “other mechanisms,” his concerns were resolved. *Id.* at 77:4-6. Mr. Ruemmler expressly disavowed Plaintiffs’ view that the WAA button limitation “saved to your Google Account” extends to pseudonymous data. *Id.* at 101:8-10 (“When I say ‘my account,’ that means like my Google account or my—you know, associated with my GAIA ID.”); *see also id.* at 98:1-5; 108:8-110:6; 134:13-21; 227:23-229:1.

Second, Plaintiffs grossly misrepresent internal surveys of small numbers of users in long strings of single-spaced bullet points and charts. Plaintiffs chose not to conduct a user survey in this case, even though they have done so in other cases, presumably because they knew the results would not favor their preferred interpretation of the WAA control. Indeed, not a single one of these bullet-pointed snippets supports the claim that anyone has *ever* agreed that the WAA control determines whether Google can keep a receipt of ad. In particular:

- The first survey Plaintiffs rely on did not call sWAA a “loser,” it placed it in the “loser” column of a contest where 7 of 10 German respondents were confused by the *translated* text of the WAA control. *See* Opp., Dkt. 398, at 12-13 bullet 1; Mao Ex. 60, Dkt. 398-61, at -66.
- The April 2020 study presentation confirms the users understood that WAA works as advertised: that Google stops “saving all that stuff so that I wouldn’t get customized ads” and that it won’t “store *my* activity.” Mao Ex. 3, Dkt. 398-4, at -11.
- The 2017 presentation stating that WAA is “not well understood” confirms that **users *did understand*** that WAA determines whether data is associated with the user’s account, but did *not* uniformly understand how turning WAA *on* would personalize their experience. *See* Mao Ex. 66, Dkt. 398-67, at -706.
- The 2019 presentation is irrelevant; it studied whether users understood the interaction of WAA and data retention settings Google was testing; it concluded that some users wanted to be able to customize the number of months WAA data was retained. *See* Mao Ex. 67, Dkt. 398-68, at -82.
- The “Key Insights” spreadsheet Plaintiffs rely on is inscrutable and they cherry-pick a single line with no real content. Mao Ex. 68, Dkt. 398-69.
- The reference that “WAA isn’t clear to users” in Mao Ex. 69, Dkt. 398-70, at -239 is

meant to convey that the name “Web & App Activity” is not by itself descriptive, and some users skipped over the page in Android inviting them to customize how long WAA data would be retained.

- Arne de Booij’s hypothesis designing a user study, *see* Opp., Dkt. 398, at 12-13 bullet 5; Mao Ex. 41, Dkt. 398-42, at -99.R, showed that Google expended effort to try to prevent users racing through account creation in Europe. Dr. de Booij testified that the study focused on account creation for European users, not on WAA, and that his hypothesis was to be tested, not taken as true. *See* Santacana Dec. at Ex. E (de Booij Tr.) at 99:5-6, 100:21-101:5.
- The general comment in Mao Ex. 65, Dkt. 398-66, at -680, *see* Opp., Dkt. 398, at 12-13 bullet 7, continues to express concern around making the WAA disclosures as clear as possible, but does not endorse Plaintiffs’ interpretation of WAA.
- Jens Mueller’s concern was about the *Dutch translation* of English text he considered sufficiently clear, and Dave Monsees’ response was that WAA is described at a *level of technical vagueness so that it is accurate to users* (since the technical complexities could unnecessarily and inaccurately alarm users). *See* Opp, Dkt. 398, at 3:17; Mao Ex. 1, Dkt. 398-2.
- J.K. Kearns never agreed with Plaintiffs’ position. *See* Opp., Dkt. 398, at 12-13 bullet 2. He worked on Google Search, and expressed the opinion that when users turn off WAA, data collected when WAA was on should not be used to personalize search results. *See* Mao Ex. 61, Dkt. 398-62, at -14; Santacana Dec. at Ex. F (Kearns Tr.) at 41-42, 86-87, 96.
- Nor did Kearns agree with Plaintiffs in his July 2020 email, *see* Opp., Dkt. 398, at 12-13 bullet 6, where he and Monsees expressed concern that a popular Android feature that shows on-device search history would interact strangely with WAA being turned off because turning WAA off would either break the search history feature, angering users, or it wouldn’t affect it, confusing users. *See* Mao Ex. 64, Dkt. 398-65, at -81.R & 82.R; Santacana Dec, at Ex. F (Kearns Tr.) at 86 (testifying that his comment related to whether data should be saved to a user’s Google Account when WAA is off).
- Brenda Chen’s comment, *see* Opp., Dkt. 398, at 12 bullet 3; Mao Ex. 62, Dkt. 398-63, relates to an unknown document and unknown issue, and nobody was questioned on it.
- The unknown March 2020 comment similarly lacks context (*see* Opp., Dkt. 398, at 12-13 bullet 4); its author and meaning are unknown, and nobody was questioned about it, nor does it address any aspect of Plaintiffs’ claims.

None of these documents raise a dispute of material fact because they do not address anything close to Plaintiffs’ interpretation of what WAA meant vis-à-vis GA4F data; some of them relate to a completely different language, and all relate to completely different functionality. Even if these studies could create ambiguity about some uses of WAA-off data, they are irrelevant to the specific data types and uses at issue in *this* case.

III. Plaintiffs cannot establish a reasonable expectation of privacy, intent, or highly offensive conduct.

1 The Court’s Order allowing certain claims to proceed was premised on the allegation,
 2 taken as true, that Google was collecting sWAA-off users’ “browsing habits and histories” and
 3 “detailed URL requests, app browsing histories, and search queries” through GA4F. Order
 4 Regarding MTD, Dkt. 109, at 16. Relying on the Ninth Circuit’s decision in *In re Facebook*, the
 5 Court held that such tracking, if proven, could support Plaintiffs’ claims for invasion of privacy
 6 and violation of CDAFA. But discovery debunked that theory. *Id.* At summary judgment, without
 7 any evidence of offensive tracking that could violate a reasonable expectation of privacy, the
 8 Court should reject Plaintiffs’ claims as a matter of law. Indeed, the sum of the certified theory of
 9 liability is that Google’s logs keep a record that a pseudonymous ID was shown a particular ad,
 10 kept only for record-keeping, in violation of a reasonable expectation of privacy.

11 Far from denying this absurdist view of the law, Plaintiffs’ brief doubles down on it. They
 12 feebly attempt to distinguish cases like *Low*, *McCoy*, *Williams*, *London*, and *Hammerling* while
 13 relying on inapposite decisions far afield from the undisputed facts to argue that users have a
 14 reasonable expectation of privacy in de-identified data.⁵ And in *Brown v. Google LLC*, 2023 WL
 15 5029899 (N.D. Cal. Aug. 7, 2023), on which Plaintiffs heavily rely, the Court purported to rely on
 16 the Ninth Circuit’s decision in *Campbell v. Facebook, Inc.*, 951 F.3d 1106, 1119 (9th Cir. 2020),
 17 but that case expressly disavowed the *Brown* Court’s view, noting in footnote 9: “We emphasize
 18 that this case also does not present the question whether standing could be based entirely on injury
 19 from anonymized, aggregated uses of data.” Further, the *Brown* Court was deciding only the
 20 question of Article III standing, and the *Campbell* panel distinguished standing because the
 21 question of whether there’s a reasonable expectation of privacy in anonymous data is “merits
 22 arguments in disguise” which “tell us nothing about whether Plaintiffs had standing.” *Id.*

23 And even if Plaintiffs are right that Google failed to describe the complexities of its system
 24 perfectly, it does not follow that Google intentionally invaded users’ privacy; though Google’s
 25 system design was intentional, it was intentionally designed to deidentify (s)WAA-off data
 26 according to Google’s reasonable understanding of what the WAA control meant. To hold Google
 27

28 ⁵ See, e.g., *Wesch v. Yodlee, Inc.*, 2021 WL 1399291, at *3 (N.D. Cal. Feb. 16, 2021) (holding *at pleading stage* that selling *inadequately deidentified* information was actionable).

1 liable because it may have failed to find the perfect words to speak to its one billion users around
2 the world stretches the common law too far.

3 Regardless, Google’s conduct here—attempting to but allegedly failing to perfectly
4 capture the scope of the WAA button to reflect that Google does keep pseudonymous logs of the
5 ads it serves—could not possibly be highly offensive. *See, e.g., In re Zynga Priv. Litig.*, 750 F.3d
6 1098, 1108 (9th Cir. 2014) (no reasonable expectation of privacy in record information about
7 communications); *In re Google, Inc. Privacy Pol’y Litig.*, No. 5:12-CV-001382-PSG, 2015 WL
8 4317479, at *6 (N.D. Cal. July 15, 2015) (“This district sets a high bar for the requisite intrusion
9 that is highly offensive.”); *I.C. v. Zynga, Inc.*, 600 F. Supp. 3d 1034, 1049 (N.D. Cal. 2022)
10 (“[T]he discovery of a password to a gaming account” is not “highly offensive to a reasonable
11 person, particularly where there is no allegation that the gaming accounts for which plain text
12 passwords were taken contain confidential information.”); *McCoy v. Alphabet, Inc.*, 2021 WL
13 405816, at *8 (N.D. Cal. Feb. 2, 2021) (collection of anonymized, aggregated data on frequency
14 and duration of app usage “does not rise to the requisite level of an egregious breach of social
15 norms”); *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1063 (N.D. Cal. 2012) (disclosure
16 of device identifier, personal data, and geolocation information “does not constitute an egregious
17 breach of social norms”). Plaintiffs’ response on this point is pure rhetoric, spuriously accusing
18 Google of trying to defraud users with fake controls, even though it is undisputed the (s)WAA
19 control does, in fact, make a significant difference in how Google processes the data in question,
20 and that Google created an infrastructure at its own expense to effectuate that understanding of
21 what the control should do. Finally, Plaintiffs argue that because Google profits from anonymized
22 data, its collection of the data *must be* highly offensive. That argument is facially baseless.

23 **IV. Plaintiffs cannot establish harm.**

24 Keeping a digital receipt that an ad was served to a de-identified user does not harm
25 anyone. *See Spokeo, Inc. v. Robins*, 578 U.S. 330 (2016) (holding that a plaintiff must allege a
26 concrete injury, not just a bare procedural violation, to satisfy Article III standing); *Low*, 900 F.
27 Supp. 2d 1010, 1032 (N.D. Cal. 2012) (finding no “appreciable, nonspeculative, present injury”
28 where plaintiffs failed to allege “how either Plaintiff was foreclosed from capitalizing on the value

1 of his personal data” and noting that “although Plaintiffs theorize that third parties could de-
 2 anonymize this data, it is not clear that anyone has actually done so”); *Massie v. Gen. Motors*
 3 *LLC*, No. CV 21-787-RGA, 2022 WL 534468, at *5 (D. Del. Feb. 17, 2022) (“possession of
 4 anonymized, non-personal data regarding [plaintiffs’] browsing activities on GM’s website [did
 5 not harm] their privacy interests in any way”). Plaintiffs’ arguments that they suffered harm
 6 cannot withstand the reasonable juror test. Further, to secure class certification of a damages class,
 7 Plaintiffs presented specific damages calculations. *See* Class Cert. Order, Dkt. 352, at 2-3 (laying
 8 out Plaintiffs’ damages models). They cannot now rely on other sources of harm to satisfy the
 9 harm elements of their claims. To do so would be to backtrack on their renunciation of, for
 10 example, emotional harms or other non-uniform harms, which inherently require individualized
 11 inquiries. *See* Pltfs’ Class Cert. Reply, Dkt. 333 (“Google faults Plaintiffs for . . . failing to offer a
 12 fifth method of calculating monetary relief, based on emotional distress. The law does not require
 13 plaintiffs to offer methodologies for every theoretical measure of relief.”).

14 The argument that a bare privacy harm is sufficient to maintain either the tort claims or the
 15 CDAFA claim is wrong. Both claims *require* actual harm, not just the bare Article III harm of
 16 invasion of privacy. CACI 1820 (2024) (listing damages for intrusion upon seclusion as “[m]ental
 17 suffering/anxiety/humiliation/emotional distress,” and special damages); BAJI 7.26 (2024) (listing
 18 damages based on “harm to plaintiff’s interest in privacy resulting from the invasion,” “mental or
 19 emotional distress caused by the invasion” and economic losses plaintiff “has sustained to date, or
 20 is reasonably certain to suffer in the future”). And though an *individual* plaintiff might be able to
 21 maintain such a claim based on the emotional harm that comes from an invasion of privacy, the
 22 class here cannot. Plaintiffs’ argument that the harm elements are satisfied by damage to battery
 23 life suffers from the same problem, as well as another: Plaintiffs never presented a damages
 24 methodology based on this supposed harm at class certification; if they are to survive summary
 25 judgment on that basis, they would be disabled from arguing at a class trial that they can recover
 26 damages for that harm, and so their damages class must be decertified.

27 The remaining harms Plaintiffs put forward are all the same, and boil down to an argument
 28 that because Google profited, Plaintiffs must have been harmed (even though by their own

admission, they would not have sold the data in question if they could, nor does Google’s collection of it stop them from selling the data to any willing buyer for the exact price they’d otherwise obtain on the open market). The problem with this argument is that it is no longer good law, as Judge Chhabria has acknowledged. *See McClung v. AddShopper, Inc.*, 2024 WL 189006 (N.D. Cal. Jan. 17, 2024). Plaintiffs label Judge Chhabria’s holding dicta. It is not, but it doesn’t matter. His reasoning, keying off of *TransUnion*, 594 U.S. at 426–30, is sound and makes common sense. That a defendant may profit does not mean the plaintiff has suffered any harm in particular. Harmless data collection can be profitable just as the harmless failure to redact all but the last six digits of a credit card number on a receipt does not mean the credit cardholder has suffered any concrete harm. *Ellsworth v. Schneider Nat’l Carriers, Inc.*, 2021 WL 6102514, *5 (C.D. Cal. Oct. 28, 2021) (finding no standing even where “credit report was published to a third party,” and that “harm is an injury in law—and ‘an injury in law is not an injury in fact’”) (citing *TransUnion*, 594 U.S. at 2205); *Gadomski v. Patelco Credit Union*, 2022 WL 223878, at *5 (E.D. Cal. Jan. 25, 2022) (no “concrete injury in fact” where Plaintiff failed to demonstrate present or future harm from inaccurate credit report). Simply put, an “interest in preventing Defendants from enjoying ill-gotten profits is not an injury in fact,” much less the actual harm required for the tort and CDAFA claims. *Winsor v. Sequoia Benefits & Ins. Servs. LLC*, No. 21-CV-00227-JSC, 2021 WL 5053087, at *5 (N.D. Cal. Nov. 1, 2021), *aff’d*, 62 F.4th 517 (9th Cir. 2023). But Plaintiffs’ damages methodologies presented at class certification are purely based on disgorgement of profit, not on a reduction in any economic interest Plaintiffs had in their data. *See* Dkt. 364-17 (Lasinski Tr.), at 286:17-287:10 (acknowledging his model has no basis in data’s quantity or nature).

Finally, no reasonable juror can conclude that any plaintiff was deprived of an economic opportunity to *sell* data that Google took for free. Plaintiffs’ theory is that they did *not* wish to sell the data in question. And even if they wanted to, no record evidence suggests the value of the data was diminished or that Google’s conduct disabled them from selling it.⁶ As a result, there is no class-wide evidence in the record concerning this question.

⁶ Plaintiffs’ “benefit of the bargain” harm is confusing; this Court dismissed their contract claim. And no damages theory was presented on this score at class certification.

1 **V. Conclusion**

2 For the foregoing reasons, the Court should grant summary judgment to Google.

3
4 Dated: June 13, 2024

Respectfully submitted,
WILLKIE FARR & GALLAGHER LLP

6
7 By: /s/ Eduardo E. Santacana

8 Benedict Y. Hur
9 Simona Agnolucci
10 Eduardo E. Santacana
11 Argemira Flórez
12 Harris Mateen

13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
Attorneys for Defendant
Google LLC